+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 16/12/2025

S'inscrire

Formation Préparation à la Certification Microsoft Azure AZ-5OO

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Presentation

Maîtrisez la sécurisation des charges de travail sur Microsoft Azure avec la préparation AZ-500. Apprenez à réduire les surfaces d'attaque, à automatiser les contrôles et à répondre aux exigences de conformité. Idéale pour protéger vos applications, données et identités dans des environnements hybrides et cloud natif.

À l'issue de cette formation, vous saurez concevoir une architecture Zero Trust, implémenter l'accès conditionnel, le RBAC et PIM, segmenter le réseau avec NSG/ASG et Azure Firewall, protéger les données via Key Vault et le chiffrement, puis durcir la posture avec Azure Policy.

La formation privilégie les ateliers guidés, labs reproductibles et démos pas-à-pas. Des cas d'usage IaaS, PaaS et conteneurs ancrent chaque compétence.

Objectifs

- Évaluer les risques et définir une stratégie Zero Trust sur Azure.
- Implémenter et durcir l'identité et les accès (MFA, accès conditionnel, RBAC, PIM).
- Sécuriser réseaux et workloads (NSG/ASG, Azure Firewall, WAF).
- Protéger secrets et données (Key Vault, chiffrement, SAS).
- Surveiller, détecter et répondre aux menaces (Defender for Cloud, Sentinel, Log Analytics).

Public visé

- Ingénieurs Cloud / DevOps
- Administrateurs systèmes et sécurité
- Architectes cloud

Pré-requis

- Bases d’Azure (ressources, groupes de ressources, VNet, Storage).
- Notions de sécurité réseau et IAM.
- Pratique de PowerShell ou Azure CLI.
- Lecture d’anglais technique.

Pré-requis techniques

- Ordinateur 64 bits avec 8–16 Go de RAM.
- Windows 10/11, macOS ou Linux.
- Accès Internet stable et navigateur moderne.
- Compte Azure avec rôle Contributor (ou sandbox fournie en session).
- Outils installés : Visual Studio Code, Azure CLI, PowerShell (module Az).

Programme de notre formation Microsoft Azure AZ-5OO

[Jour 1 - Matin]

Fondamentaux de la sécurité Azure et Zero Trust

- Responsabilité partagée, principes Zero Trust et cartographie des risques
- Mesurer la posture avec Microsoft Defender for Cloud et Secure Score
- Gouvernance sécurité : RBAC, balises, Azure Policy (initiatives, remédiation)
- Bonnes pratiques de segmentation, accès privé et réduction de surface d’attaque
- Atelier pratique : Audit express d’un abonnement et plan d’actions priorisé

[Jour 1 - Après-midi]

Identités et contrôle d’accès avec Microsoft Entra ID (Azure AD)

- Rôles Entra ID vs RBAC Azure : portées, bonnes pratiques de délégation
- Accès conditionnel, MFA, durcissement des sessions et protections de base
- PIM (Just-In-Time) pour rôles et groupes privilégiés
- Comptes de service et Identités managées pour accès aux ressources
- Atelier pratique : Configurer PIM et une stratégie d’accès conditionnel

[Jour 2 - Matin]

Protection réseau et segmentation

- Conception VNet, sous-réseaux, peering et routage (UDR)
- Contrôles : NSG/ASG, Azure Firewall (DNAT/SNAT, règles d’application)
- Exposition sécurisée : Private Link/Endpoints, Private DNS, Service Endpoints
- Périmètre : WAF (Application Gateway) et DDoS Protection
- Atelier pratique : Segmenter un VNet et publier une appli via WAF et Private Link

[Jour 2 - Après-midi]

Sécuriser la couche plateforme : VM, PaaS et conteneurs

- Durcissement des VM : Update Management, Guest Configuration, chiffrement de disque
- PaaS sécurisé : App Service/Functions (restrictions IP, VNet integration, Managed Identity)
- Sécurité des conteneurs : AKS, ACR, analyse d’images et Defender for Containers
- Sauvegarde, verrous (resource locks) et restauration comme filet de sécurité
- Atelier pratique : Activer Defender, scanner des images ACR et bloquer un déploiement non conforme

[Jour 3 - Matin]

Collecte des logs, KQL et alerting

- Sources : Activity Log, Diagnostic Settings et tables Log Analytics
- Ingestion avec Data Collection Rules et séparation des espaces de travail
- Requêtes KQL pour recherche, agrégations et visualisations
- Alertes, Action Groups et automatisation avec Logic Apps
- Atelier pratique : Créer un tableau de bord et des alertes KQL orientées sécurité

[Jour 3 - Après-midi]

Détection et réponse avec Microsoft Sentinel

- Déploiement de Sentinel et connecteurs de données (Azure, M365, Syslog)
- Règles d’analytique, corrélation et gestion des incidents
- Automatisation SOAR : playbooks Logic Apps et réponses guidées
- Hunting : requêtes KQL, signaux anormaux et bonnes pratiques d’investigation
- Atelier pratique : Enquêter un incident et automatiser une réponse

[Jour 4 - Matin]

Protection des données, clés et secrets

- Chiffrement au repos/en transit : SSE avec CMK, Azure Disk Encryption
- Key Vault : RBAC vs stratégies, pare-feu/réseau privé, soft-delete et purge protection
- Sécurité Storage : RBAC, clés partagées, SAS, immutabilité (Blob)
- Accès “secretless” avec Managed Identities pour apps et workloads
- Atelier pratique : Déployer un Key Vault, rotater un secret et lier une appli via Managed Identity

[Jour 4 - Après-midi]

Sécurité applicative et préparation à l’examen

- App Service/Functions : AuthN/AuthZ intégrée, restrictions réseau, secrets
- DevSecOps : scans de code/dépendances, secrets scanning et gates de sécurité en CI/CD
- Conformité continue : Azure Policy (deny, DeployIfNotExists), évaluation et remédiation
- Révision finale : domaines de compétences, pièges fréquents et plan d’entraînement

Passage d'un examen blanc

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte

des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.